Many Advances Made, But Additional Emphasis Is Needed on Key Initiatives in the Security Services Organization

October 2002

Reference Number: 2003-20-005

INSPECTOR GENERAL
for TAX
ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

October 4, 2002

MEMORANDUM FOR DEPUTY COMMISSIONER FOR MODERNIZATION &
CHIEF INFORMATION OFFICER

Pamela J. Gardiner

FROM: Pamela J. Gardiner
Acting Inspector General

SUBJECT: Final Audit Report - Many Advances Made, But Additional Emphasis Is Needed on Key Initiatives in the Security Services Organization (Audit # 200220022)

This report presents the results of our review of key initiatives in the Security Services organization. The overall objective of this review was to evaluate the effectiveness of selected activities performed by the Security Services organization. We undertook this review to assist us in making our annual evaluation of the Internal Revenue Service's (IRS) technology security program and practices.

In summary, a successful security program relies on both the managers in the IRS' business units and the Chief Information Officer's (CIO) staff to develop and enforce security policies. Office of Management and Budget (OMB) policy states that functional managers are primarily responsible for the security of systems under their control. The CIO's office must administer the program by coordinating with managers in business units to provide a strategic view of the agency's crosscutting security needs. In the IRS, this function is carried out by Security Services.

Since its establishment in 1997, Security Services has been responsible for increasing the attention given to technology security issues within the IRS. Security Services has made many significant advances including a much stronger virus protection program, the establishment of the Computer Security Incident Response Center, effective efforts made in response to the terrorist activities of September 11, 2001, and subsequent anthrax attacks, improvements made in IRS-wide disaster recovery capabilities, particularly at the computing centers, and increasing the number of systems that have been certified. Significant progress has also been made in establishing a Common

Operating Environment to standardize software and security features on employees' computers.

Still, we believe Security Services could continue to improve security in the IRS by placing more emphasis on a few key areas. Increased emphasis in the areas noted below will help to ensure that computer security controls are being effectively implemented and operating as intended to reduce risks.

- Policies for some key security issues have not been developed. Those policies that have been developed have taken up to several years before being issued. The IRS remains unnecessarily vulnerable to security attacks while these policies are being developed.
- Security Services did conduct reviews of key IRS facilities during the year. However, Federal law requires functional managers to annually review the security of the systems for which they are accountable. To our knowledge, none of these reviews were conducted. Security Services officials believed that their facilities reviews achieved the intent of the law. Without the annual system reviews, however, the IRS has only limited assurance that the appropriate policies and procedures have been developed and implemented and that system controls integrate with other IRS systems.
- While Security Services uses various methods and techniques to provide computer security awareness, it does not have a systematic method for evaluating whether these activities are having a positive effect. Having such information would enable Security Services management to better direct its computer security awareness activities to the topics and audiences that need the most attention.
- The computer security training program needs improvement. Until recently, Security Services had deferred to business unit managers to ensure that required training took place and to a group of Information Systems personnel in the Midwest area to develop curricula. Although recommended by standards-setting organizations, computer security training in the IRS is not role-based, a system is not in place to accurately track the training employees attend, and methods do not exist to determine whether employees have learned, retained, and applied what they have been taught. Based on our limited sample, employees may not be receiving adequate training. As a result, systems may be unnecessarily at risk.

Security Services developed an effective monitoring tool to help track progress on these and other key security issues. Actions were initiated to reduce security vulnerabilities in each of 15 areas. Quarterly reviews are conducted to evaluate progress and to highlight specific areas needing further improvement.

We recommended that resources be assigned to develop policies for key security issues and that the process for vetting policies be streamlined. Upfront involvement by functional users could expedite the approval process. Functional managers should

conduct annual system reviews to comply with the Government Information Security Reform Act (GISRA) and Security Services should assist, using tools mandated by the OMB. Security Services should develop techniques to gain feedback on awareness activities and develop a more formal training program for employees with key security responsibilities.

Management's Response: Security Services management disagreed with recommendations #1 and #2, stating that policies already exist for many of the areas that we indicated need to be developed and that their policy vetting process is sufficient as it now exists. They partially agreed with recommendations #3 and #4, indicating that actions are underway over the next 18 months to identify and define the roles and responsibilities of functional officials for conducting annual systems reviews. However, Security Services believes its current technical assessments, which include some systems reviews, substantially reduce the risks of functional officials not fulfilling their GISRA responsibilities for conducting annual assessments of their sensitive systems.

Management agreed with our other recommendations. Security Services is implementing an employee survey to better target future security awareness efforts. Also, actions are being taken to have Security Services, in partnership with other relevant functions, identify, define, and track competency-based security training.

Office of Audit Comment: Although Security Services indicates that policies do exist for seven of the nine areas indicated in our report, the references provided do not include clear policy statements. We concur with the MITRE study, which concluded that well-developed and publicized policies in these areas need to be completed. In addition, implementation of security policies has taken, in some cases, years to be developed. As noted in the report, for example, guidance for administering the Windows NT operating system used throughout the IRS took several years to develop. We anticipate that the policy development process should improve with the implementation of the Security Governance structure initiated during our audit.

Furthermore, we believe that 18 months is too long to clarify the responsibilities of functional officials for evaluating the security of their systems. The IRS is nearly 2 years behind in implementing the GISRA requirements in this area. The GISRA has already clarified the responsibilities of functional officials. It states that functional officials should use the National Institute of Standards and Technology self-assessment guidelines in making those evaluations. We do not intend to elevate these disagreements to the Department of the Treasury for resolution.

Copies of this report are also being sent to the IRS managers who are affected by the report recommendations. Please contact me at (202) 622-6510 if you have questions or Scott E. Wilson, Assistant Inspector General for Audit (Information Systems Programs), at (202) 622-8510.

Table of Contents

Many Advances Made, But Additional Emphasis Is Needed on Key Initiatives in the Security Services Organization

Background

Federal law and policy state that functional managers are primarily responsible for the security of their systems and must assess the risks for each of those systems. The Chief Information Officer (CIO) is responsible for administering the security program and providing a strategic view of security issues that cut across these systems. In the Internal Revenue Service (IRS), this responsibility has been given to the Chief, Security Services.

Security Services (formerly the Office of Security) was established in 1997 to create corporate solutions for Agency-wide computer security problems. Security Services' responsibility is to focus on a continuous program of evaluating and improving the IRS' security program and processes and to work with management to drive solutions, develop sound security processes, and establish mechanisms that support IRS functional managers in assessing security risks and making decisions regarding those risks.

Evaluating and improving security in the IRS is a difficult challenge. Unscrupulous employees may have access to sensitive taxpayer data maintained by the IRS. Also, as the primary revenue collector for the United States, the IRS is a target for both terrorists and hackers. This threat has increased with more interconnectivity of computer systems.

We performed our audit work between January and May 2002 at the Security Services office in IRS National Headquarters. The audit was conducted in accordance with *Government Auditing Standards.* Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

Security Services Has Taken Action to Strengthen the Overall Program

Since its inception in 1997, Security Services has focused increased attention on the issue of computer security within the IRS. Its primary focus has been to address issues that have posed significant security risks for the IRS. For example:

- Corrective actions were taken that resulted in a much stronger virus protection program.

- The Computer Security Incident Response Center has significantly enhanced the intrusion detection efforts within the IRS.
- Security controls were enhanced at all IRS campuses in response to the terrorist activities of September 11, 2001, and subsequent anthrax attacks. Related improvements have been made in IRS-wide disaster recovery capabilities, particularly at the computing centers.
- The number of systems that have been certified has increased. As of May 2002, the IRS reported that 39 percent of its systems had been certified, ensuring that they contain appropriate security controls necessary to protect against system breaches. While this is still a relatively low percentage, progress has been made since 2000, when only 10 percent of its systems were certified.
- A major effort has been made to ensure security features are included in new systems before they are "rolled out."
- A significant effort has been made to implement the Common Operating Environment (COE) that provides IRS end-users with a uniform set of applications and common software features. The COE provides a means to affect what an end-user can and cannot do, by enabling or disabling specific features of the operating system and computer applications.

Overall, Security Services has made significant strides in addressing security issues, particularly with a limited staff. However, additional improvements are needed in the following key areas.

Security Policy Development Needs to Be Streamlined

In February 2002, the IRS asked the MITRE Corporation to provide an analysis to identify gaps between Federal/Department of the Treasury requirements and IRS security policies. MITRE identified policy gaps in 12 areas including the following:

- Continuity of Operations Plans.
- Classified Systems.
- Credit Card Security on the Internet.
- Electronic Signatures.
- Financial Management System Controls.
- Internet mechanisms, including CGI Scripts and ActiveX.[1]
- Storage and Labeling of Limited Official Use Data.
- Records Management.
- Threat Coordination.

The IRS has begun work on the Continuity of Operations Plans. However, policies have not been developed to address the other policy gaps.

The development of policies often takes an unreasonable length of time, even for critical security issues. For example, guidance for administering the Windows NT operating system used throughout the IRS took several years to develop. The IRS is estimating that critical policies over the configuration of Internet gateways, which control information to and from the Internet, will take 15 months to issue from the date the need to do so was identified.

A policy for the Intrusion Detection System and firewalls is also taking an unreasonable amount of time to develop. The MITRE Corporation, under another contract, had delivered guidance, standards, and procedures in February 2002. The Deputy Director, Computer Security for Incident Response, is now in the process of making some changes and updates to that guidance. The guidance will then undergo the vetting process and then be submitted to the Technology Security Committee headed by the Deputy Commissioner for Modernization & CIO. Final guidance is now expected to be delivered by September 2002 but could take even longer.

[1] CGI scripts represent software used by Internet sites to execute various applications. ActiveX controls contain computer code designed to work through Internet Explorer browsers. The interactive components of these controls expose the applications and files on workstations to viruses.

We attribute these policy gaps to a lack of emphasis by Security Services and to an unnecessarily lengthy vetting process used by the IRS. Guidelines have to go through a process whereby all the affected parties in the IRS review the guidelines and offer their concerns, problems, and suggestions that Security Services then tries to address. The vetting process takes months.

While the policies and guidance are being developed, the vulnerabilities and risks are still left unresolved. Computer security issues change rapidly with additional risks and exposures to IRS systems occurring daily. The process of policy development and implementation should be streamlined to keep pace and afford protection of systems and infrastructure.

Recommendations

The Deputy Commissioner for Modernization & CIO should:

1. Assign the necessary resources to address the critical policy gaps and accelerate estimated completion dates for draft policies and guidance.

Management's Response: Management, in effect, disagreed with this recommendation by stating that policies existed for many of the areas that we indicated need to be developed.

Office of Audit Comment: Although Security Services indicates that policies do exist for seven of the nine areas indicated in our report, the references provided do not include clear policy statements. We concur with the MITRE study, which concluded that well-developed and publicized policies in these areas need to be completed.

2. Accelerate the vetting process. We recognize that input from functional users is critical to the success of all security policies. Rather than wait until guidance is drafted, we suggest that user representatives be assigned early to assist in the development of the policies. The vetting process could also be accelerated by establishing and adhering to tight time frames for review and comment.

Management's Response: Management, in effect, disagreed with this recommendation by stating that their policy vetting process is sufficient as it now exists.

Office of Audit Comment: Implementation of security policies has taken, in some cases, years to be developed. As noted in the report, for example, guidance for administering the Windows NT operating system used throughout the IRS took several years to develop. We anticipate that the policy development process should improve with the implementation of the Security Governance structure initiated during our audit.

Program Officials Do Not Conduct Required Annual Program Reviews

Security Services' oversight responsibilities have been assigned to Security Policy Support and Oversight. This office carries out these responsibilities primarily by conducting physical security checks, automated network scans, and other facilities-based reviews. Between May 2001 and April 2002, it conducted 27 reviews of IRS facilities and performed network reviews at 10 service centers. The system reviews were limited to the use of scanning software. Weaknesses were identified and recommendations to improve security were made.

The Government Information Security Reform Act (GISRA) also requires that appropriate senior functional officials annually test and evaluate information security controls and techniques on the systems assigned to them. The Office of Management and Budget (OMB) states that the CIO should assist functional officials in understanding and addressing risks, especially the increased risk resulting from interconnecting with other programs and systems over which the functional officials have little or no control. The OMB suggests that, to promote consistent reviews and reporting across the government, functional officials should use the CIO Council's Federal Information Technology Security Assessment Framework and National Institute of Standards and Technology (NIST) guidance as a basis.

IRS business unit officials had not conducted any security reviews in Fiscal Years (FY) 2001 and 2002, to date. Security Services did not play an active role in encouraging and assisting in these reviews because it believes that it meets the intent of the GISRA through its facility reviews.

The Chief, Security Services, believes that the office's methodology provides a more comprehensive, enterprise-wide approach for assessing the IRS' security programs than would be provided by using a system-by-system approach.

Security Services also believes that the GISRA and OMB guidance are subject to many different interpretations and that the OMB did not provide sufficient or timely guidance to agencies to clarify expectations. Security Services did not believe the OMB intended agencies to apply the review guidance to each IRS sensitive system.

We followed up with the OMB and confirmed it intended that each system be reviewed annually using the NIST framework. The OMB clarified this issue in guidance issued for GISRA reporting in FY 2002.

We believe that both the facility reviews conducted by the IRS and the annual system reviews required by the OMB are necessary to determine the acceptable level of risk and to maintain an adequate level of security. Facility reviews give some assurance of the adequacy of physical, operating system, and network security. However, without the sensitive system reviews, the IRS cannot fully assess whether security policies and procedures have been consistently implemented, and if operational, management and technical controls are functioning as intended for its sensitive systems.

Conducting annual system reviews should promote accountability for functional executives and ensure that security controls enable, but do not unnecessarily impede, business operations.

Recommendations

The Deputy Commissioner for Modernization & CIO should:

3. Require responsible functional officials to assess each agency-wide system at least annually to comply with existing law and policy. Functional officials should develop action plans for all sensitive application

weaknesses and coordinate with Security Services to correct those weaknesses. Per the OMB, the scope of the annual reviews can vary depending on risk, prior reviews, and the status of corrective actions for previously identified system weaknesses.

Management's Response: Security Services has activities underway to identify and define the roles and responsibilities of the functional officials for conducting annual system reviews, in partnership with the business units. Management anticipates addressing this issue over the next 18 months. However, Security Services believes its current technical assessments, which include some systems reviews, substantially reduce the risks of functional officials not fulfilling their GISRA responsibilities for conducting annual assessments of their sensitive systems.

Office of Audit Comment: We believe 18 months is too long to implement these actions since the IRS is already nearly 2 years behind in implementing the GISRA requirements in this area. In addition, the GISRA has already clarified the responsibilities of functional officials. It states that they should use the NIST self-assessment guidelines in conducting the annual evaluations of their systems.

4. Assist functional managers in complying with the intent of GISRA and OMB requirements by:
   - Participating with functional officials in conducting the required annual program reviews. To meet this responsibility, it may be necessary to divert some resources currently used by Security Policy Support and Oversight in its facility reviews.
   - Including the results of the program reviews in the annual self-assessment provided to the Department of the Treasury.
   - Including the weaknesses identified in the program reviews in the Plan of Action and Milestones.

Management's Response: Management is making improvements to comply with GISRA and OMB requirements. Activities are underway to identify and define the roles and responsibilities of the functional

officials for conducting annual program assessments, in partnership with the business units. As functional officials implement the defined roles and responsibilities, their results will be included in the annual self-assessment and Plan of Action and Milestones provided to the Department of the Treasury. Management anticipates addressing these issues over the next 18 months.

Security Awareness Activities Are Not Evaluated

Another function of Security Services is to promote security awareness for all IRS employees. The Security Awareness Program Office is charged with carrying out this responsibility. We consider employee awareness of security risks to be perhaps the weakest link in protecting taxpayer data and assets from disclosure or loss. For example, in a prior TIGTA review,[2] 71 of 100 employees we contacted were willing to change their password to 1 provided by a caller pretending to work on the Help Desk.

Security Services has provided a wide variety of computer security awareness activities using various methods and techniques as recommended by the NIST and the General Accounting Office (GAO). However, it does not have assurance that its efforts are having a positive effect.

Security Services does not have a systematic method for regularly obtaining information or data on the impact of its computer security awareness activities. Such information could be used to evaluate the effectiveness of these activities, help measure trends in whether employee computer security awareness is improving or decreasing, and help redirect computer security awareness activities to the topics and audiences that need the most attention.

The NIST and the GAO recommend that computer security awareness activities include:

- Using test measures, such as true/false or multiple-choice questions, to ascertain what has been learned and retained.

[2] *Management Advisory Report: Network Penetration Study of Internal Revenue Service Systems* (Reference Number 2002-20-057, dated March 2002).

- Using incident reports to monitor for noncompliance with computer security.
- Observing how well employees follow recommended security procedures.
- Conducting periodic tests by contacting employees directly to measure their security awareness.

Another potential source for analyzing trends in employee computer security awareness is the IRS' Automated Labor and Employee Relations Tracking System (ALERTS). The ALERTS contains a database of employee relation cases that may result in disciplinary and adverse actions. The ALERTS coding system tracks cases involving unauthorized access to tax return or return information and misuse of the Internet and e-mail systems.

Security Services does not use any of these methods to evaluate the effectiveness of its computer security awareness activities. Security Services officials advised that the IRS generally does not test employees to determine what they have learned or retained from training. They advised that their responsibility ends with providing the awareness, with the only testing accomplished during the periodic compliance reviews conducted by Security Policy, Support and Oversight.

By not tracking and evaluating its security awareness efforts, the IRS cannot determine whether employees understand their security responsibilities. Employees could commit security breaches knowingly or unknowingly that result in loss or unauthorized disclosure of taxpayer data. Also, awareness activities may not be targeted to the appropriate audience, which could result in unnecessary costs.

Recommendation

To better assess the effectiveness of computer security awareness activities, the Deputy Commissioner for Modernization & CIO should:

5. Consider testing security awareness by surveying selected employees as part of the annual computer

security awareness week activities, performing direct contact tests to assess employees' awareness of computer security, reviewing data available in the ALERTS and incident reports to identify trends, and targeting awareness activities to those trends.

Management's Response: Management will explore various assessment methods and techniques for evaluating the effectiveness of their computer security awareness activities. The Security Awareness Program Office will continue to develop and improve tools for obtaining feedback on computer security awareness activities and responding with targeted awareness activities. The School of Information Technology (SIT) is improving its ability to identify trends, and the Security Awareness Program Office will work closely with security officers to develop annual security awareness training that employees receive. Management anticipates addressing these issues over the next 18 months.

Security Services Has Not Effectively Overseen the Computer Security Training Program

The NIST and the GAO recommend that:

- Computer security training should be role-based. Role-based learning focuses on the job functions employees perform rather than on their job titles. It provides security training that satisfies the specific requirements of an employee's role.
- A system for effectively tracking each employee's training should be in place.
- Methods should be employed for determining whether employees have learned and retained what they have been taught and whether their performance has improved. Some of the better methods that can be used to help measure this are various types of testing that take place before and at the end of courses and feedback from supervisors on whether employee performance has improved.

IRS employees with key security responsibilities are dispersed in many locations throughout the organization. Many report to the Deputy Commissioner for Modernization & CIO, but others report to functional managers. Ensuring that each of these employees receives the appropriate training for his or her role is a difficult

challenge. Currently, IRS computer security training does not follow any of the NIST and GAO recommendations.

Curricula for key security roles have not been developed. The SIT operated by the Midstates Area had begun developing employee skill sets based on the job functions employees perform and with the intent of identifying specific training that will provide employees the needed skills. These initiatives have no formal or approved plans that set forth the tasks to be performed, the persons assigned to these tasks, time frames for completing them, and expected deliverables. Without the expertise and vision of employees in Security Services, we believe it a high risk that the training will not be on target.

In addition, a reliable system is not in place to track employees' training. The IRS uses a national database for storing training data on employees; however, the data are not kept current. As a result, the IRS cannot determine the number of employees given security training, the types of training provided, and the costs of the training. Plans are not in place to replace this system.

Also, testing and other follow-up techniques are not used to determine whether training was successful. The IRS cannot determine whether employees have learned and retained what they have been taught and whether their performance has improved.

As a result, Security Services has no assurance that employees are adequately skilled to perform computer security duties, which could place systems at unnecessary risk.

Security Services had not sufficiently overseen, directed, and guided these initiatives. Instead, it had deferred to the SIT for the development of the security training program. Functional managers submitted their training requests directly to the SIT.

Security Services believed that functional managers were in the best position to decide their staffs' training needs and assumed that these managers provided it. Security Services placed the responsibility on the managers for being aware of their staffs' current assignments and ensuring that the

training received was commensurate with the employees' assignment and put into practice immediately. Security Services also believed that correcting the training database was not its responsibility.

Near the end of our review, Security Services committed to defining those skills necessary for employees with security responsibilities and assisting in devising curricula for acquiring needed skills. We still believe that Security Services is in the best position to also oversee and track training to ensure a consistent skill level is maintained for these key employees.

Recommendation

The Deputy Commissioner for Modernization & CIO should:

6. Take overall responsibility for providing security training. Curricula should be developed for each key security role. Consideration should be given to requiring annual minimum continuing professional education credits. Training given to employees with key security responsibilities should be tracked, and methods for determining whether employees learn and retain what they have been taught need to be developed and used.

Management's Response: Management has activities underway to identify, define, and track competency-based security training. These activities will identify security-related training needs of defined security roles, validate and update courses, communicate training opportunities and guidance to key personnel, complete development of e-learning tools, and begin quarterly monitoring of course participation. Management anticipates addressing these activities over the next 18 months. The SIT is improving its ability to identify participation and trends through the service-wide training system it maintains. Additional employee security training assessment tools and methods will require coordination with the National Treasury Employees Union.

Security Services Has Developed a Process to Monitor Progress in Meeting Security Objectives

Security Services developed a framework that identifies the key security responsibilities of Federal agencies. It is linked to the 15 security areas provided by the NIST. The framework, if used effectively, enables management to quickly identify the current status, barriers to improvement, responsible official, and expected completion date for corrective actions. The IRS has identified actions to reduce security vulnerabilities in each of the 15 areas and is tracking its progress during quarterly business performance reviews. The Department of the Treasury adopted the IRS' framework for use in all bureaus.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this audit was to evaluate the effectiveness of selected activities performed by the Security Services organization. We undertook this review to assist us in making our annual evaluation of the Internal Revenue Service's (IRS) security program and practices, as required by the Government Information Security Reform Act (GISRA). We expect many of the questions posed by the Office of Management and Budget (OMB) for the 2002 GISRA process to be centered on the activities of Security Services.

To accomplish our overall objective, we performed work on the following five sub-objectives:

I. Determined if Security Services provided the policies and procedures necessary to protect IRS data, personnel, and equipment.

   A. Obtained the MITRE Corporation's security policy and procedure gap analysis.

   B. Obtained the IRS' response to MITRE's findings in the analysis and reviewed corrective actions proposed by the IRS. Determined if the response contained specific assignment of actions needed along with expected completion dates.

   C. Based on other audit work, the Chief Information Officer (CIO) Council's Federal Information Technology Security Assessment Framework, and guidance issued by the National Institute of Standards and Technology (NIST), determined if there were any policies and procedures not identified by MITRE's policy and procedures gap analysis.

II. Determined if Security Services provided sufficient direction to functional executives in carrying out its required annual reviews and had adequate controls to monitor such reviews.

   A. Identified applicable OMB requirements for the annual reviews.

   B. Contacted the OMB and ascertained its intent regarding who is to perform the reviews and the review scope.

   C. Determined Security Services' understanding of OMB requirements regarding the annual reviews.

   D. Documented the extent to which the annual reviews had been conducted by functional executives.

   E. Documented the system that Security Services has in place to ensure that the reviews are performed.

   F. Identified instructions and requirements that Security Services had provided to

functional executives in carrying out their annual required reviews. Determined if the basis for these instructions and requirements was the CIO Council framework consisting of five questions for each sensitive system. Determined if:

1. The instructions required functional executives in coordination with Information Technology Services staff to annually review their risk assessments and security plans and system configuration settings for the systems they own.
2. The instructions were consistent with GISRA requirements for assigning responsibilities for accomplishing the required annual reviews.

III. Determined if Security Services provided sufficient direction on the types of training needed for specific security functions, and determined if it adequately monitored the delivery to ensure all security employees received the necessary training.

A. Obtained back-up documentation supporting the assessment and rationale for the training performance criteria assertions.

B. Obtained the tactical plan for the training assertions.

C. Compared the plan to NIST and Office of Personnel Management guidance on computer security training.

D. Interviewed key personnel for the training tactical plan.

E. Selected a sample of 20 employees with security responsibilities and obtained documentation to determine if they have had the required training.

IV. Determined if Security Services had taken sufficient actions to increase IRS employees' awareness of their security responsibilities. Determined if:

A. Security Services had a designated organizational component responsible for carrying out computer security awareness activities.

B. There were standardized consequences for security violations.

C. The awareness training program included communicating to users the consequences of committing security violations.

D. Security Services was aware of violations that had occurred, and if so, determined what disciplinary actions were taken in these cases.

E. Listed all security awareness actions and compared them to NIST guidelines on implementing a good security awareness program.

V. Determined if Security Services had performed sufficient tests to ensure that security policies and procedures were implemented as prescribed.

A. Identified Security Evaluation and Oversight's responsibilities for conducting periodic security control reviews at IRS facilities. Researched the Internal Revenue

Manual and other applicable guidance.

B. Obtained a schedule of reviews planned and completed by type of facility for the last 2 fiscal years.

C. Compared the scope of its reviews with guidance provided by the CIO Council framework and NIST guidance.

D. Determined if it documented weaknesses identified in these reviews in its database and if it followed up to ensure the weaknesses were corrected

.

Appendix II

Major Contributors to This Report

Scott E. Wilson, Assistant Inspector General for Audit (Information Systems Programs)
Stephen Mullins, Director
Gerald H. Horn, Audit Manager
Richard T. Borst, Senior Auditor
Bret D. Hunter, Senior Auditor
David C. Hodge, Auditor
Joan Raniolo, Auditor

Appendix III

Report Distribution List

Commissioner N:C
Deputy Commissioner N:DC
Chief, Security Services M:S
Chief Counsel CC
National Taxpayer Advocate TA
Director, Legislative Affairs CL:LA
Director, Office of Program Evaluation and Risk Analysis N:ADC:R:O
Office of Management Controls N:CFO:F:M
Audit Liaisons:
Deputy Commissioner for Modernization & Chief Information Officer M
Office of Security Services M:S

Appendix IV

Management's Response to the Draft Report

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, D.C. 20224

RECEIVED
SEP 23 2002

SEP 23 2002

MEMORANDUM FOR TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

FROM: Len Baptiste
Chief, Security Services

SUBJECT: Response to Draft Audit Report – Many Advances Made But Additional Emphasis is Needed on Key Initiatives in the Security Services Organization (Audit # 200220022)

Protecting taxpayer information and ensuring the integrity of our information systems are two of the most critical important tasks of the Internal Revenue Service (IRS). During this time of heightened security, we have taken aggressive action to prevent potential security breaches. In addition, we understand that all employees have a role in protecting our systems and we are continuing to work with all IRS offices to better define their roles and emphasize the importance of following security policies and procedures.

In general, we agree with many of the findings which are included in your draft report. They are consistent with continuing IRS actions to strengthen its security capabilities and safeguard taxpayer data. As acknowledged in your report, the IRS has strengthened its security capabilities in a number of areas. For example, it has:

- Corrected numerous physical, systems, and network security weaknesses identified during systems and facilities reviews performed by the General Accounting Office, the Treasury Inspector General for Tax Administration and Security Services;
- Developed a security assessment framework, corrective action plans and approaches to better focus and prioritize continuing efforts to correct weaknesses;
- Established an effective 24X7 computer security incident response capability (CSIRC);
- Refocused efforts to adequately address the increased risks associated with last year's terrorist attacks;
- Implemented an improved systems security certification process, which resulted in an increasing number of sensitive systems being certified; and
- Developed security standards for operating systems and telecommunications.

In 2001, the GAO reported that computer security was a continuing high-risk area throughout the federal government. It also noted that the IRS was an agency that had taken significant steps to improve security capabilities, including correcting a significant number of identified weaknesses and establishing an agency wide computer security management program that should, when fully implemented, help it to effectively manage its security risks. Actions addressed by the program have been timely given that more time-critical priorities (e.g., modernization and post September 11, 2001 actions) had to also be addressed throughout the last few years. In this regard, we disagree with your report's finding that policy-setting issues are not being adequately or timely addressed. The MITRE study referenced in your report, that identified security policy gaps, was proactively initiated by Security Services to improve policies. Similarly, the IRS' establishment of a security governance structure, consisting of three executive committees, was initiated to ensure that senior leadership participated in a more timely process to adopt and implement security polices.

Ongoing efforts to correct the IRS' computer security material weakness, includes aggressively defining and implementing the systems security roles and responsibilities of the operating divisions, Information Technology Services and Security Services. Whereas, we agree with your report's finding that functional managers have a responsibility to review their systems, we believe that Security Services will continue to provide the technical assessments needed to support their responsibility. In this regard, the technical expertise to support such reviews was assigned to Security Services when it was first established in 1997 so that this limited technical expertise could be leveraged to provide guidance and support to functional and systems management across the Service. We also believe that until functional managers' roles and responsibilities are defined and implemented, the risks associated with them not doing these reviews have been mitigated by ongoing Security Services reviews. These activities will proceed as quickly as possible, as will efforts to enhance our security awareness and training programs. Barring any unforeseen incidents, which could result in a shift of resources to address other more time-critical risks, it is anticipated that these issues will be addressed over the next 18 months. More detailed responses to your recommendations are included in the attachment.

If you have any questions, please call me at (202) 622-8910, or Rose Hernandez, Director, Security Policy Support and Oversight at (202) 283-4500.

Attachments (2)

Attachment I

Management Response to Draft Audit Report
Many Advances Made But Additional Emphasis Is Needed on Key Initiatives in the Security Services Organization (Audit # 200220022)

RECOMMENDATION #1:

The Deputy Commissioner for Modernization & Chief Information Officer should assign the necessary resources to address the critical policy gaps, and accelerate estimated completion dates for draft policies and guidance.

ASSESSMENT OF CAUSE:

Actions have been underway to address this issue. Critical policy gaps identified by MITRE and reported by TIGTA do not exist. Security Services engaged MITRE to perform a traceability analysis to identify both the links and gaps between authoritative Federal and Department of Treasury security requirements and the IRS Internal Revenue Manual (IRM) 25.10.1. There may have been a misinterpretation by the TIGTA auditors of the information they reviewed from the MITRE analysis that caused them to believe that this analysis included all IRMs. As indicated on the attached matrix, IRS has existing policies for seven of the nine areas delineated in the audit report as needing to be developed (see Attachment II). The IRS will continue to use the Security Governance structure to adopt and implement security policies.

CORRECTIVE ACTION TO RECOMMENDATION #1:

The IRS has been actively addressing this issue. As TIGTA reported, the policy for Continuity of Operations Plans is being developed in conjunction with new direction provided by the Office of Homeland Security and Treasury. Currently, the IRS does not have a business need for Electronic Signatures, and as such, there is no need for the policy. However, Security Services is a key player with Electronic Tax Administration and the Business Systems Modernization Office in determining when this capability will be needed. Security Services will ensure that the appropriate policy is in place when needed.

IMPLEMENTATION DATE:

Completed

RESPONSIBLE OFFICIAL:

Director, Security Policy Support and Oversight

Attachment I

RECOMMENDATION #2:

The Deputy Commissioner for Modernization & Chief Information Officer should accelerate the vetting process. We recognize that input from functional users is critical to the success of all security policies. Rather than wait until guidance is drafted, we suggest that user representatives be assigned early to assist in the development of the policies. The vetting process could also be accelerated by establishing and adhering to tight timeframes for review and comment.

ASSESSMENT OF CAUSE:

Actions have been underway to address this issue. During TIGTA's audit, the IRS implemented the Security Governance structure which consists of many of the attributes in TIGTA's recommendation. The security governance structure, which consists of three Executive committees, to ensure that senior leadership participates in a more timely and responsible process to implement security policies. These committees consist of membership throughout the Service to ensure that proposed policies are adequate from both a security and business perspective, and can be properly and consistently implemented at the operational and user levels throughout the Service. A recent example of the utility of this governance process was the development, vetting, and subsequent approval for the Windows 2000/XP Security Standards. This process ran from April through August 2002, and included partners and stakeholders from IRS Security Services, Information Technology Services, and various business units; as well as participation from the U.S. General Accounting Office and TIGTA. The Windows 2000/XP Security Standard has been approved by the Technology Security Committee as an interim policy pending completion of the document clearance process for final publishing in the IRS Law Enforcement Manual, as section 25.10.7.

CORRECTIVE ACTION TO RECOMMENDATION #2:
The IRS will continue to use the Security Governance process to adopt and implement security policies. Security Services will ensure that policy consideration is brought to the appropriate Committee in a timely fashion. Therefore, the IRS does not agree with TIGTA's assertion that our policy vetting process is ineffective.

IMPLEMENTATION DATE:
Completed

RESPONSIBLE OFFICIAL:
Director, Security Policy Support and Oversight

Attachment I

RECOMMENDATION #3:

The Deputy Commissioner for Modernization & Chief Information Officer should require responsible functional officials to assess each agency-wide system at least annually to comply with existing law and policy. Functional officials should develop action plans for all sensitive application weaknesses and coordinate with Security Services to correct those weaknesses. Per the OMB, the scope of the annual reviews can vary depending on risk, prior reviews, and the status of corrective actions for previously identified system weaknesses.

ASSESSMENT OF CAUSE:
Functional officials do not have, within their organizations, the technical resources capable of conducting annual reviews of their systems. In addition, the roles and responsibilities for conducting annual security reviews have not been defined for functional officials.

CORRECTIVE ACTION TO RECOMMENDATION #3:
IRS partially concurs with this recommendation. Although IRS functional managers have a responsibility to assess their systems for adequate controls, this requirement is partially fulfilled through the technical assessments conducted by Security Services. These assessments include the determination of the adequacy of physical, systems and network controls, as well as disaster recovery capability. The results of these assessments are provided to, and corrective action plans are developed with Information Technology Services, which is independent of Security Services. The technical expertise needed to support such reviews was assigned to Security Services when it was established in 1997, so that its limited technical expertise could be leveraged to provide guidance and support to functional and systems management across the Service. In this regard, until functional managers' roles and responsibilities for conducting annual system reviews are identified, defined and implemented, the risks associated with them not doing these reviews continue to be mitigated by ongoing Security Services' reviews.

In conjunction with the IRS material weakness corrective action plan and the Model Facility initiative led by Security Services, activities are underway to identify and define the roles and responsibilities of the functional officials in partnership with the business units. Barring any unforeseen incidents, which could result in a shift of resources to address other more time-critical risks, it is anticipated that this issue will be addressed over the next 18 months.

IMPLEMENTATION DATE:
April 2004

RESPONSIBLE OFFICIAL:
Director, Security Policy Support and Oversight

RECOMMENDATION #4:

The Deputy Commissioner for Modernization & Chief Information Officer should assist functional managers in complying with the intent of GISRA and OMB requirements by:

- Participating with functional officials in conducting the required annual program review. To meet this responsibility, it may be necessary to divert some resources currently used by Security Policy Support and Oversight in its facility reviews.

- Including the results of the program reviews in the annual self-assessment provided to the Department of the Treasury.

- Including the weaknesses identified in the program reviews in the Plan of Action and Milestones.

ASSESSMENT OF CAUSE:
The specific roles and responsibilities for conducting annual system assessments have not been defined for functional officials.

CORRECTIVE ACTION TO RECOMMENDATION #4
The IRS has actions underway to address this issue. Although IRS functional managers have a responsibility to assess their systems for adequate controls, the IRS has already fulfilled most of this requirement through the security vulnerability assessments conducted by Security Services. These assessments include the determination of the adequacy of physical, systems and network controls, as well as disaster recovery capability. The technical expertise needed to support such reviews was assigned to Security Services, so that its limited technical expertise could be leveraged to provide guidance and support to functional and systems management across the Service. However, improvements in the IRS' compliance with GISRA and OMB requirements are being taken. Barring any unforeseen incidents, which could result in a shift of resources to address other more time-critical risks, it is anticipated that the following issue will be addressed over the next 18 months:

- In conjunction with the IRS material weakness corrective action plan and the Model Facility initiative led by Security Services, activities are underway to identify and define the roles and responsibilities of the functional officials in partnership with the business units.

- As the functional officials implement the defined roles and responsibilities for conducting annual program assessments, their results will be included, along with the results of the technical assessments by Security Services, in the annual self-assessment provided to the Department of Treasury.

- As the functional officials implement the defined roles and responsibilities for conducting annual program assessments, their results will be included, along with the results of the technical assessments by Security Services, in the Plan of Action and Milestones provided to the Department of Treasury.

IMPLEMENTATION DATE:
April 2004

RESPONSIBLE OFFICIALS:
Director, Security Policy Support and Oversight
Business Operating Divisions
Functional Operating Divisions

Attachment I

RECOMMENDATION #5:

To better assess the effectiveness of computer security awareness activities, the Deputy Commissioner for Modernization & Chief Information Officer should consider testing security awareness by surveying selected employees as part of the annual computer security awareness week activities, performing direct contact tests to assess employees' awareness of computer security, reviewing data available in the ALERTS and incident reports to identify trends, and targeting awareness activities to those trends.

ASSESSMENT OF CAUSE:
Assessment methods need to be developed and/or improved to better measure the effectiveness of computer security awareness activities.

CORRECTIVE ACTION TO RECOMMENDATION #5:
The IRS concurs with this recommendation and will explore various assessment methods and techniques. The Security Awareness Program Office, in conjunction with the MITS Human Resources School of Information Technology (SIT), will continue to develop and improve tools for obtaining feedback on computer security awareness activities and responding with targeted awareness activities. For example, an on-line survey was developed and utilized for the 2001 Security Awareness Week activities. This survey is currently being improved and will be available to capture employee feedback during the November 2002 Security Awareness Week and again in December 2002. The SIT is responsible for tracking training, and is improving its ability to identify participation and trends through the service-wide training systems it maintains. Business unit managers are responsible for ensuring that employees receive annual security awareness training. The Security Awareness Program Office will continue to work closely with security officers in the field to develop this annual training.

In conjunction with the IRS material weakness corrective action plan and the Model Facility initiative led by Security Services, activities are underway to identify and define competency-based security training in partnership with the SIT, Information Technology Services, and business units. Barring any unforeseen shift of resources to address other more time-critical risks, it is anticipated that this issue will be addressed over the next 18 months.

IMPLEMENTATION DATE:
April 2004

Attachment I

RESPONSIBLE OFFICIALS:
Director, Mission Assurance
School of Information Technology
Information Technology Services

RECOMMENDATION #6:

The Deputy Commissioner for Modernization & Chief Information Officer should take overall responsibility for providing security training. Curricula should be developed for each key security role. Consideration should be given to requiring annual minimum continuing professional education credits. Training given to employees with key security responsibilities should be tracked and methods for determining whether employees learn and retain what they have been taught need to be developed and used.

ASSESSMENT OF CAUSE:

A security curriculum, that is also tracked for student participation, is not implemented Service-wide.

CORRECTIVE ACTION TO RECOMMENDATION #6:

IRS concurs with this recommendation. In conjunction with the IRS material weakness corrective action plan and the Model Facility initiative led by Security Services, activities are underway to identify, define and track competency-based security training in partnership with the MITS Human Resources School of Information Technology (SIT), Information Technology Services, and business units. Barring any shift of resources to address other more time-critical risks, it is anticipated that the following activities will be addressed over the next 18 months.

- Identify security-related training needs to correspond to defined security roles and responsibilities.
- Validate and update current on-line and classroom courses for key personnel.
- Periodically communicate training opportunities and guidance to key personnel.
- Complete development of e-learning tool for key personnel to correspond with defined security roles and responsibilities.
- Begin quarterly monitoring of curriculum course participation.

The SIT is responsible for tracking employee training, and is improving its ability to identify participation and trends through the service-wide training systems it maintains. Additional employee security training assessment tools and methods will also require coordination with the National Treasury Employees Union (NTEU). The business unit managers are responsible for ensuring that employees receive security awareness training.

Attachment I

IMPLEMENTATION DATE:
April 2004

RESPONSIBLE OFFICIALS:
Director, Mission Assurance
School of Information Technology
Information Technology Services

ATTACHMENT II

Management Response to Draft Audit Report
Many Advances Made But Additional Emphasis Is Needed on Key Initiatives in the Security Services Organization
(TIGTA Audit # 200220022)

AREAS MITRE IDENTIFIED AS POLICY GAPS	EXISTING IRS POLICY	IRM OWNER
Continuity of Operations Plan	Under development as reported	Security Services
Classified Systems	IRM 1.9 published	Agency-wide Shared Services (AWSS)
Credit Card Security on the Internet	Purchase Card Guide (Doc.9185) (Internet Purchases)	AWSS
Electronic Signatures	No existing IRS business need	N/A
Financial Management Systems Controls	• Financial Management Guide (February 1997) • AFS Reference Guide (May 1998) • AFS Runbook • AFS Queries Pocket Guide • AFS On-line User's Guide • RTS/AFS User's Guide	Chief Financial Officer
Internet Mechanisms, including CGI Scripts and ActiveX	IRM 25.10.1.7.9.1(2)	Security Services
Storage & Labeling of Limited Official Use Data	IRM 1.16.8.2-5	AWSS
Records Management	IRM 1.15.1 & 2	AWSS
Threat Coordination	SAMC Procedures	Security Services/AWSS/ Security Executive Steering Committee/ Operations Security Committee